Tóth Gábor

AZ IOT-ESZKÖZÖK[1] JELENTETTE TERRORFENYEGETÉS

TERRORIZMUS – KIBERTERRORIZMUS

A mindennapi életünk folyamatos digitalizációja a terrorizmus egy új fajtáját hozta létre, a kiberterrorizmust. Mikortól beszélhetünk kiberterrorizmusról? Mi is a kiberterrorizmus? Ha a terrorjellegű cselekményeket az internet segítségével hajtják végre, vagy az interneten?

Ahhoz, hogy a fenti kérdésekre választ találjunk, először is a terrorizmus fogalmát kell megvizsgálnunk. A különböző szerzők más aspektus szerint közelítik meg a terrorizmus meghatározását. Benjamin Netanjahu szerint: „A terrorizmus a békés polgárok elleni szándékos, módszeres erőszak, amely az általa kiváltott félelmen keresztül politikai célokat kíván megvalósítani."[2]

A fenti fogalom alapján láthatjuk, hogy az erőszak egy kulcsfontosságú tényező, amit mi sem bizonyít jobban, mint hogy a 2012. évi C. törvény a Büntető Törvénykönyvről 314–316. §-a szerinti terrorcselekmény törvényi tényállását megvizsgálva, láthatjuk, hogy a „Btk. 314. § (1) bekezdésében megjelölt első alapeset elkövetési magatartásai azonosak a (4) bekezdésében felsorolt, személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekmények (eszközcselekmények) elkövetési magatartásaival. Ez utóbbi bűncselekmények a speciális célzat (terrorista cél) révén minősülnek terrorcselekménynek, ennek hiányában azonban megmaradnak önálló köztörvényes bűncselekményeknek, betöltve saját funkciójukat a Btk. rendszerében."[3]

Más szóval az interneten végrehajtott kibertámadásoknak hatást kell kiváltaniuk a fizikai világban. Korábban ilyen jellegű cselekményeket nehezen lehetett elképzelni, sci-fi-filmekben találkozhattunk ezekkel, de napjainkra valósággá váltak.

A kiberterrorizmus kifejezés a fejlett információs technológia romboló célokra történő szándékos felhasználását jelenti. Korábban a kiberterrorizmus hagyományos

[1] Internet of Things: dolgok internete.

[2] Netanjahu 1995: 20.

[3] Kasznár 2017: 95.

DOI: https://doi.org/10.36250/01259_16

módszerei kevésbé voltak károsak, most viszont egy teljesen új dimenziót öltöttek, amely halálos természetű is lehet.[4]

Az ismert és használt fogalmaink alapján az első olyan jellegű kibertámadásra, amely a fizikai világban is hatást váltott ki, 2010-ben a Stuxnet botnet volt képes, amikor az iráni urándúsítású centrifugák ellenőrzésére használt programozható logikai vezérlőket támadták meg.

Adam Henschke arról írt 2021-ben, hogy még nem történt olyan kibertámadás, vagy legalábbis nem ismert, amely a fizikai világban konkrét hatást váltott volna ki a Stuxneten kívül. Igaz, az internetet – vagy más szóval a kiberteret – a terroristák rendkívül kifinomultan használják toborzásra, radikalizálódásra és propagandára, de az Iszlám Állam még a csúcspontján sem tudott olyan jellegű támadást végrehajtani az internet segítségével, amely fizikai hatást váltott volna ki.

Ez alapján Henschke a kiberterrorizmust kétféleképpen közelíti meg. Az első megközelítése szerint ha a kiberterrorizmus során az internetet félelemkeltésre vagy politikai, ideológiai célok elérésére használják, akkor propagandáról vagy információs műveletekről beszélünk. Bruno Halopeau szerint a terrorista szervezetek általában propagandacélokra használják az internetet. A világméretű web és a web 2.0 folyamatos fejlődése lehetőséget biztosított a nyilvánosság számára az információk egyszerű elérésére és közzétételére magas szintű informatikai ismeretek nélkül is.[5]

Henschke másik megközelítése szerint a kiberterrorizmus során a terroristák az internetet és az azokhoz kapcsolt eszközöket arra használják fel, hogy a fizikai világban erőszakos módon változást idézzenek elő.

Hogy szemléltetni tudjam a különbséget, nézzünk meg két példát. Az első példánál a terrorista csoport az interneten keresztül küld egy üzenetet, amely arról szól, hogy kárt fognak okozni. Ez Henschke felosztása szerint az első csoportba tartozik.

A másik példa szerint a terrorista csoport akciót szervez, amelynek keretein belül autonóm járművek informatikai rendszerét hackelik meg, és ezeket a járműveket összehangolt támadásra használják fel, akár gyalogosok ellen, akár más, kiemelt fontosságú létesítmény ellen. Majd ezt követően a terroristák az interneten keresztül azt kommunikálják, hogy ők a felelősek a támadásokért, és ha a követeléseiket nem teljesítik, további ilyen támadásokra lehet számítani.

A példák alapján különbséget tudunk tenni a két megközelítés között, amelyek során az egyiknél csak kommunikációra használják fel az internetet, míg a másik esetben konkrét támadást hajtanak vele végre.[6]

[4] Husain–Khan 2020: 15.
[5] Akhgar–Staniforth–Bosco 2014: 123.
[6] Henschke et al. 2021: 73.

Fontos tényezőként ki kell emelni az ilyen támadásoknál az erőszakos jelleget. Ugyanis egy másik példával élve – amely ugyan hatást váltott ki a fizikai világban, de nem volt erőszakos – 2022-ben a Yandex taxitársaságot feltörték Moszkvában, ami közlekedési káoszt okozott, viszont erőszakos jellegű cselekmény nem történt. Ez az a példa, amely alapján a hacktivizmust és a kiberterrorizmust el lehet határolni. Az utóbbi példában leírt cselekményt hacktivizmusnak lehet nevezni, azonban ha erőszakos jellegű cselekményt is végrehajtottak volna, akkor beszélhetnénk kiberterrorizmusról.

Annak oka, hogy korábban miért nem volt hasonló támadásokra példa, és hogy napjainkra miért adatott meg a lehetőség, az információs technológiában keresendő. Az IoT-eszközök megjelenésével megteremtődtek a feltételek, hogy a valós fizikai világ és a számítógépek, illetve az internet között kialakuljon egy kapcsolat, amely hídként köti össze őket.

IOT-ESZKÖZÖK JELENTETTE TERRORFENYEGETÉS

Mik azok az IoT-eszközök?

Napjaink kihívásai között kiemelt szerepet kapnak az IoT-eszközök, ezek az úgynevezett „okos" eszközök. Ha le szeretnénk fordítani az IoT, azaz Internet of Things kifejezést, talán úgy lehetne, hogy a „Dolgok Internete", azonban ez egy nem igazán megfogható fogalom így.

Mielőtt a különböző szerzők és szervezetek által meghatározott fogalmakat bemutatnám, fontosnak tartom, hogy az informatika világában csak felhasználóként jelen levők is pontosan értsék, hogy mit is jelent ez a rövidítés. Az IoT-eszközök azok az eszközök, amelyek kölcsönhatásba lépnek különféle számítógépes eszközökkel, például mobiltelefonokkal, táblagépekkel. Az IoT-eszközök a legtöbb esetben nem függetlenek, a kommunikációs hálózatok sebessége és a beprogramozott vagy általuk megtanult szabályok befolyásolják működésüket. Megjelenési formájuk egészen szerteágazó, az egyszerűbb megjelenési formáik között megemlíthetők a hőmérséklet-érzékelők, de bonyolultabb rendszereket is alkothatnak, amire a legjobb példák az intelligens járművek.[7]

Fontos kihangsúlyozni, hogy ezeknek az eszközöknek kapcsolatba kell lépniük a környezetükkel, amelyről adatokat kell szolgáltatniuk a felhasználóknak vagy a további rendszereknek, de a környezetükben változást is képesek előidézni.

[7] Boye 2019: 15.

Egy egyszerűbb rendszer esetében, amely kifejezetten csak a külső hőmérsékletet figyeli, elég lehet a felhasználó számára egy visszajelzés, de egy okosotthon tekintetében, amely egy bizonyos hőmérséklet felett automatikusan nyitja vagy zárja az ablakokat, nem elég csak a felhasználónak küldött visszajelzés, jelen esetben a központi rendszernek is továbbítani kell adatokat, amely az ablakok nyitásáért és zárásáért felelős.

Felhasználási helyüket tekintve mindennapi életünk megkönnyítésében és az iparban a termelés ellenőrzésében és javításában is fontos szerepet játszanak.

Az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (European Union Agency for Cybersecurity – ENISA) szerint az IoT „egy olyan széles ökoszisztémát ír le, ahol az egymással összekapcsolt eszközök és szolgáltatások adatokat gyűjtenek, cserélnek és dolgoznak fel annak érdekében, hogy dinamikusan alkalmazkodjanak a kontextushoz”.[8] Boye szerint az

> „IoT eszközöknek alapfeltétele és célja, hogy azok az eszközök, melyek jelenleg nem kapcsolódnak számítógépes hálózatba, nevezetesen az internethez, kapcsolódjanak, hogy kommunikálni tudjanak és interakcióba tudjanak lépni az emberekkel és más eszközökkel. Az IoT egy technológiai átmenetet képez, amelyben az eszközök lehetővé teszik számunkra a fizikai világ érzékelését és irányítását azáltal, hogy az eszközöket intelligensebbé teszik és intelligens hálózaton keresztül kapcsolják őket össze.”[9]

Az IoT-eszközök története

Az IoT-eszközök 2008 és 2009 körül kezdtek kialakulni, ebben az időszakban több „okos”-eszköz csatlakozott fel az internetre, mint ahány ember.

Az Internet of Things meghatározást először Kevin Ashton használta 1999-ben, amikor a Procter & Gamble-nél dolgozott. Ezzel a kifejezéssel mutatta be új ötletét, amelynek segítségével rádiófrekvenciás azonosítókat és egyéb érzékelőket helyezett el a cég ellátási láncában lévő termékekre. Az elhelyezett eszközök adatokat szolgáltattak arról, hogy a termékek a raktár mely polcain találhatók, vagy eladták-e őket.[10]

Kevin Ashton véleménye szerint a 20. században a számítógépek csak azt tudták végrehajtani, amit beléjük programoztak, érzékelésre alkalmas eszközökkel nem

[8] *ENISA Threat Landscape Report 2017.*
[9] Boye 2019: 15.
[10] Elder 2019.

rendelkeztek, a 21. században a számítógépek különböző érzékelőkkel vannak már felszerelve, amivel saját maguk gyűjtik be az információkat.

Az 1990 után globálissá váló internet napjainkig tartó folyamatos fejlődését négy szakaszra lehet osztani. A fejlődés során az egyes szakaszokat markánsan nem lehet elkülöníteni, ugyanis azok egymásra épültek.

Az első szakasz az 1990-es évekre tehető, amikor még nem volt minden háztartásban internet, ebben az időszakban leginkább az e-mail-küldés volt a jellemző.[11]

Az internet fejlődésének második szakaszáról onnantól beszélhetünk, hogy az internethez való csatlakozás nem okozott problémát, a felhasználók elkezdték kiaknázni az általa nyújtott lehetőségeket. Erre az időszakra tehető az online kereskedelem megjelenése is, ahol a termelők, a beszállítók és a fogyasztók közvetlenebb viszonyba kerültek egymással.

A harmadik fázisról akkor beszélhetünk, amikor a személyek közötti kapcsolattartás és kapcsolatteremtés elkezdett digitalizálódni. Ebben a szakaszban már intenzíven jelen van a közösségi média, a Facebook, az Instagram, a Twitter és még sok más alkalmazás. Ezen időszak másik fontos tényezője a mobilitás lett, különféle eszközök jelentek meg, amelyek mobilissá tették az informatikai eszközöket.[12]

A negyedik szakasz az eszközök internethez és egymáshoz való kapcsolódásáról szól, ez a folyamat zajlik napjainkban is. Ezek a kapcsolatok új kihívások elé állítják az informatika szakembereit, tekintettel az adatok mennyiségére. Gondoljunk bele, minden eszköz, amely kapcsolódik egymáshoz vagy az internethez, adatot közvetít. Példaként nézzünk egy napjainkban gyártott új autót, amely a vezető számára az abroncsok levegőnyomásától kezdve a GPS[13] használatáig hasznos információkat szolgáltat, amelyeket tárolni kell, és a vezetőnek hozzáférhetővé kell tenni.

Az IoT-eszközök felépítése

Az IoT-eszközök jelentette kihívások, kockázatok és fenyegetések értékelése szempontjából elengedhetetlen, hogy ismerjük ezeknek az eszközöknek a felépítését a megfelelő megítélés érdekében.

Maguk az eszközök elektronikusak vagy elektromechanikaiak, amelyek közvetlenül kapcsolatba lépnek környezetükkel, és különböző feladatokat látnak el, ilyen az érzékelés, a működtetés, a számítási műveletek végzése és a kommunikáció.[14]

[11] HANES et al. 2017: 49.
[12] HANES et al. 2017: 50.
[13] Global Positioning System: Globális Helymeghatározó Rendszer.
[14] BOYE 2019: 15.

Az érzékelési műveletek alapján az eszközök képesek információt gyűjteni a környezetükből. Ilyen információk lehetnek a különböző fizikai, kémiai változók, a webkamerák által rögzített képek, de információkat érzékelhetnek az emberi szervezetről is, mint például a szívverés vagy a vérnyomás.

A működtetésről akkor beszélhetünk, ha az eszközt a hálózaton keresztül lehet vezérelni, vagy adatokat szolgáltat a hálózaton keresztül.

A számítási műveletek végzése kapcsán meg kell érteni, hogy ugyan az IoT-eszközök alapvetően érzékelési műveleteket hajtanak végre a rájuk írt programok alapján, azonban vannak olyan eszközök, amelyek fejlettebb számítási műveletek elvégzésére is alkalmasak.[15]

A megfelelő működés végett az eszközöknek képesnek kell lenniük kommunikálni egymással és a többi rendszerrel, amit különböző kommunikációs hálózatok segítségével képesek megoldani.[16]

Mint ahogy korábban írtam, az IoT-eszközök alapvető követelménye, hogy összekapcsolja a „való" világot a számítógépekkel. Ezen művelet során különböző adatok kerülnek az eszköz birtokába, amelyeket továbbítanak a hozzájuk csatlakoztatott eszközökhöz. Ahhoz, hogy a számítógépek tudják fogadni, és fel tudják dolgozni az adatokat, különböző szoftverekre van szükségük.

Az IoT-eszközök helyzete napjainkban

Napjainkra több millió IoT-eszközt használtak fel, amelyek szinte minden iparág területén jelen vannak, így a közlekedésben, az egészségügyben, a sportban, a szórakoztatóiparban, a nehéziparban, a gyártásban, az intelligens hálózatokban, a közüzemi szolgáltatásokban, a hőmérséklet- és környezetszabályozásban, valamint a közbiztonságban is.[17]

2017-ben a Cisco Systems azt az előrejelzést adta, hogy 2020-ra az IoT-eszközök száma el fogja érni az 50 milliárdot,[18] azonban a State of IoT 2022-es tavaszi jelentéséből kiderült, hogy az IoT-eszközök piacának növekedését továbbra is lassítja a chiphiány. 2021-ben az IoT-kapcsolatok száma 8%-kal nőtt, 12,2 milliárdra. 2022 végéig 18%-os növekedésre számítanak a szakértők, ami azt jelenti, hogy 14,4 milliárdra nő az aktív kapcsolatok száma.[19]

[15] Boye 2019: 15.
[16] Boye 2019: 15.
[17] Boye 2019: 19.
[18] Hanes 2017: 50.
[19] IoT Analytics 2022.

Ezeknek az eszközöknek alapvetően az a céljuk, hogy megkönnyítsék az életünket, a mindennapjainkat, az iparban minél több és jó minőségű terméket tudjanak előállítani kevesebb költségen. Azonban nem szabad elfelejteni, hogy ezek a fent említett, csatlakoztatott eszközök veszélyeket is rejtenek, lehetőséget teremtenek újfajta bűncselekmények megvalósítására, amelyekkel szembe kell néznünk.

Miért veszélyesek az IoT-eszközök?

Adam Henschke öt tényezőt fogalmazott meg az IoT-eszközök jelentette fenyegetések kapcsán, amelyek alapján ideálisak lehetnek egy esetleges terrortámadás elkövetésére. Fontos hangsúlyozni, hogy ezek az állítások külön-külön nem jelentenek kifejezett kockázatot, de együttes megjelenésük már igenis komoly kihívás elé állíthatja a hatóságokat. Véleménye szerint ezek:

- az IoT-eszközök kockázatos adattovábbítása;
- az IoT-eszközök jelen vannak a fizikai világban;
- az IoT-eszközök száma jelentős, amely alapján potenciális eszközökké válhatnak;
- az IoT-eszközök felhasználása során megjelenő mesterséges intelligencia;
- az IoT-eszközök nagy része „láthatatlan”. [20]

Az IoT-eszközök kockázatos adattovábbítása

A kockázat alapvető forrását maguk a felhasználók jelentik, elmondható, hogy napjainkban már nem megbízhatatlanok ezek az eszközök, de megbízhatóságuk minősége a felhasználótól függ. A megbízhatatlanság oka az IoT-eszközök alapvető felépítésében és felhasználásában keresendő. Mint ahogy az IoT-eszközök jellemzésénél is említettem, ezeknek az eszközöknek lételeme a kommunikáció. Mivel az eszközök a fizikai valós világot és a számítógépeket kapcsolják össze, az általuk gyűjtött információkat adatokként képesek továbbítani. Ezeknek az adatoknak a továbbítása megtörténhet nem biztonságos úton is. Ez potenciális veszélyt jelenthet a személyes adatok és más adatokhoz való hozzáférés tekintetében.

[20] Henschke et al. 2021: 73.

Az IoT-eszközök jelen vannak a fizikai világban

Az információs technológia folyamatos fejlődésével az IoT-eszközök egy új korszakot nyitottak meg a mindennapi életünkben. A fizikai való világba is begyűrűztek az informatikai eszközök, amelyek megkönnyítik a mindennapjainkat.

Ám emellett nem szabad elfelejtenünk, hogy a jelenlétük a terroristák számára lehetőséget biztosíthat arra, hogy egy kibertámadás kereteit túllépve fizikai erőszakot alkalmazzanak a való világban.

Erre tökéletes lehetőséget tudnak biztosítani azok a járművek, amelyek alapvetően hasznos és a biztonságos közlekedést segítő IoT-eszközökkel vannak felszerelve. Látszik az is, hogy a gépjárművek világszerte a terroristák által előszeretettel választott fegyverek, ami aggodalomra adhat okot az okosjárművek terén.[21]

Az IoT-eszközök felhasználását tekintve két csoportot különíthetünk el. Az első csoportba az ipari szintű felhasználás tartozik. Ennél a felhasználási formánál elmondható, hogy általánosságban nagyobb hangsúlyt fektetnek az adatok védelmére és az eszközök megfelelő, kiberbiztonsági szempontból biztonságos felhasználására. A másik csoportba a polgári lakosság tartozik. A polgári lakosság felhasználóiról elmondható, hogy sok esetben nem fordítanak kellő figyelmet a biztonságra, sokan úgy gondolják, hogy a terroristák az ő IoT-eszközeiket nem fogják felhasználni, illetve azt gondolják, hogy nem közölnek olyan adatokat, amelyek veszélyt jelentenének rájuk, illetve másokra.

Fontos példaként tekinthető a Strava fitneszkövető alkalmazás által közölt adatok felhasználása. A Strava egy olyan eszköz, amelynek segítségével a mozgás során, illetve az edzéseken gyűjtött adatokat lehet megosztani nyilvánosan a közösségi médiában is. Ezeket az információkat felhasználva Nathan Ruser fiatal egyetemi kutatónak sikerült beazonosítania amerikai katonai és hírszerző bázisokat. Ezeket az információkat a cég saját fejlesztésű térképhálózatán keresztül sikerült kinyerni, a felületen láthatók voltak az ellátási útvonalak, a katonák által leginkább használt épületek és a sportoláskor használt útvonaluk is.[22]

Az IoT-eszközök száma jelentős, ami alapján potenciális eszközökké válhatnak

Ahogy már korábban is szó volt róla, az elmúlt években az IoT-eszközök iránt jelentősen megnőtt az érdeklődés, ezt a folyamatosan növekvő számuk is bizonyítja mind

[21] Henschke et al. 2021: 73.
[22] Henschke et al. 2021: 78.

az ipari, mind a lakossági felhasználás tekintetében. Ám ezen számok folyamatos növekedésével az eszközökben rejlő kockázati tényező is folyamatosan növekszik.

Tekintve, hogy az IoT-eszközök nem rendelkeznek megfelelő biztonsági rendszerekkel, potenciális eszközei lehetnek egy úgynevezett botnettámadásnak.[23]

Botneteknek nevezzük az olyan, hálózatba rendeződő számítógépeket, amelyeket kártékony programmal fertőztek meg üzemeltetőjük tudta nélkül. Nevüket a robot és angolul a hálózat, azaz network szavak kohéziójából alkották meg, a köznyelvben gyakran zombigépeknek nevezik őket.[24] Ezzel a kártékony programmal túlterheléses támadásokat vagy másnéven DDoS[25]-támadásokat szoktak végrehajtani. A támadás alapvető célja, hogy ellehetetlenítse egyes eszközök vagy weboldalak elérését. A megfertőzött eszközöknek rendelkezniük kell IP-címmel, amelyet felhasználva hozzáférési kérést küldenek az oldal felé. A nagy létszámú csatlakozás miatt az adott eszköz vagy weboldal túlterhelődik, így a valós felhasználó, aki el szeretné őket érni, nem tud csatlakozni hozzájuk.

Az IoT-eszközök egy adott típusának lehetnek különböző hibái, a rosszindulatú támadók ezeket a hibákat használják ki, míg az adott eszközön lévő biztonsági rést ki nem javítják. Ez az úgynevezett zero day hiba, amelyet a gyártók egy frissítéssel orvosolni tudnak. De addig a támadók megkeresik az ilyen internetre kötött eszközöket, és azokkal hajtanak végre támadást.

Nem csak weboldalak ellen lehet túlterheléses támadást végrehajtani. Ha nagy teljesítményű eszközöket, például klímaberendezéseket egy adott területen egy adott időpontban indítanak el, manipulálni tudják az energiahálózatot. Ezt a fajta támadási formát szokás MadIoT-támadásnak nevezni. Az ilyen jellegű támadások alapvetően a villamosenergia-szolgáltatók által előre tervezett, szükséges fogyasztáshoz képest kimagaslóan magas energiafelhasználáson alapulnak. A szolgáltatók általánosságban a múltban szerzett tapasztalataik alapján tisztában vannak az adott időszakra jellemző energiaszükséglettel. A MadIoT-támadások során a támadók ezt használják ki, exponenciálisan magas energiaszükségletet idéznek elő annak érdekében, hogy a szolgáltatók ne tudják előállítani a szükséges energiát. Igaz, ilyen jellegű támadásra sem volt még példa, de 2016-ban szimulációs kísérletekkel bebizonyították, hogy igenis véghez lehet vinni ilyen jellegű támadást, amely a kritikus infrastruktúrát is képes veszélyeztetni.

[23] Henschke et al. 2021: 78.
[24] Tóth 2018: 9.
[25] Distributed Denial of Service.

Az IoT-eszközök felhasználása során megjelenő mesterséges intelligencia

Az IoT-eszközök számának jelentős növekedése mind az okosotthonokban, mind az ipari felhasználás tekintetében eredményezi, hogy szükségessé válik a mesterséges intelligencia rendszerszintű felhasználása, hogy az eszközöket teljes mértékben ki lehessen használni. A mesterséges intelligencia felhasználása lehetővé teszi az integrált rendszerek zökkenőmentes gyorsasággal való működését, amely nem igényel emberi beavatkozást.[26] Az eszközök számának növekedése következtében az általuk generált adatok mennyisége is jelentőssé válik, egyes becslések szerint ez a mennyiség napi szinten eléri a körülbelül egymilliárd GB-ot. A megnövekedett adatmennyiség el fogja érni azt a szintet, amelyet már csak a mesterséges intelligencia képes kezelni.

A mesterséges intelligencia működését tekintve matematikai és logikai alapon a már tanult folyamatokból képez le szimulációkat, és hozza meg a döntéseket. Ezen tanulási folyamat miatt lehet kifürkészhetetlennek tartani a mesterséges intelligenciát, amely a terroristák számára jó lehetőségeket biztosíthat. Önmagában nem jelentene hatalmas kockázatot, de ha a korábban ismertetett kockázati tényezőkkel együtt vizsgáljuk ezt a problémakört, már jelentős tényezőt képvisel.[27] A mesterséges intelligencia megjelenése az IoT-eszközök körében magával vonzza a dinamikus mátrixelemzés témakörét is, ugyanis ezen újfajta elemzési módszer a korábban ismert, használt elemzési és értékelési munkát új perspektívából vizsgálja meg, és lehetőséget biztosít az eszközök által begyűjtött adatok újfajta kiértékelésére.[28]

Az IoT-eszközök nagy része „láthatatlan"

Ez az állítás elsőre különös lehet, de ha belegondolunk, ezek az eszközök lassan a mindennapi életünk részévé válnak, már észre sem vesszük a jelenlétüket. A legtöbb háztartásban már megtalálhatók az IoT-eszközök, a televíziók, a biztonsági kamerák, az okosórák, az autók és minden olyan eszköz, amely csatlakozik az internethez, és adatokat oszt meg. Ezek az eszközök a technológia fejlődésének köszönhetően átalakultak, miniatürizálódtak, és szinte láthatatlanokká váltak, aminek köszönhetően a fizikai világban bárhol megtalálhatók lettek.[29]

[26] Henschke et al. 2021: 79.
[27] Henschke et al. 2021: 79.
[28] Bővebben:Bács 2022.
[29] Henschke et al. 2021: 79.

Az IoT-eszközök sérülékenysége

A folyamatosan növekvő IoT-eszközpark mind a magánháztartásokban, mind az ipari felhasználás tekintetében új kihívások elé állítja a biztonsági szakembereket. Újfajta, a hagyományos kiberbiztonságtól eltérő gondolkodásmódra és fejlesztésekre van szükség, hogy ezek az eszközök minél kevesebb problémát tudjanak okozni, illetve minél kisebb legyen az esélye annak, hogy bűncselekmény áldozatává váljanak a felhasználók, valamint minél kisebb legyen az esélye egy esetleges terrortámadás végrehajtásának.

Ugyan az IoT-eszközök egyik alapvető feladata, hogy összekapcsolja az eszközöket, de ebben rejlik az egyik legnagyobb kockázata is. Elmondható, hogy a kiberbiztonság nem egyenlő az IoT-eszközök biztonságával. A kiberbiztonsági szakemberek általánosságban a számítógépek és az azokhoz kapcsolódó rendszerek biztonságáért felelősek, viszont az IoT-eszközök az elektronika és a számítástechnika egyvelegének tekinthetők, ezért ezeknek az eszközöknek megvannak a sajátosságaik, közös elemeik ugyan vannak a számítógépekkel, de nem teljesen azok.[30]

Az IoT-eszközök felhasználása során különböző sérülékenységekkel találkozhatunk, vannak köztük egyszerűbbek és igen bonyolult felépítésűek is, fontos kiemelni, hogy ezek a sérülékenységek önmagukban nem jelentenek terrorfenyegetést, de a teljes körű megértéshez ezeket is be kell mutatni, ahogy korábban is írtam, az Adam Henschke által felállított veszélyforrások együttesen új kihívás elé állítják a hatóságokat.

Carolina A. Adaros Boye az *Understanding Cyberrisks in IoT* című művében megállapította, hogy az IoT-eszközök gyenge hitelesítőadatokkal rendelkezhetnek, előfordulhat, hogy nem biztonságos az adatkezelésük, és gyenge a hitelesítőmechanizmusuk, a felhasználók nem elég tudatosak, gyenge biztonsági szabályzattal rendelkezhetnek, a tervezés során is előfordulhatnak hibák, nyitott portokkal rendelkezhetnek, nincsenek megfelelően vagy egyáltalán nincsenek elkülönítve a kritikus komponensek, rossz fizikai biztonsággal rendelkezhetnek, rossz biztonsági konfigurációval rendelkezhetnek, adatvédelmi aggályok merülhetnek fel, nem biztonságos interfésszel rendelkezhetnek, nem biztonságos hálózati szolgáltatásokkal rendelkezhetnek.

Az első sérülékenységi faktort a gyenge hitelesítőadatok jelentik. Ahhoz, hogy egy felhasználó megfelelően tudja használni a rendelkezésre álló eszközöket, rendszereket, különféle hitelesítőadatokkal kell rendelkeznie. Ilyen hitelesítőadatok a felhasználónév és a jelszó, bár sok esetben ezeken felül is különböző hitelesítőadatokat

[30] Boye 2019: 73.

kellhet megadni.[31] A gyenge hitelesítési adatok közé azok tartoznak, amelyek alapértelmezés szerint vannak beállítva, illetve azok, amelyeket könnyen ki lehet találni. Előfordulhat olyan, hogy a gyártók által használt, alapértelmezett hitelesítési adatok kikerülnek az internetre, ami lehetőséget kínál a hackereknek, hogy különösebb erőfeszítés nélkül hozzá tudjanak férni a kiszemelt eszközökhöz. Ennek a problémának a kiküszöbölése nem csak a felhasználók feladata, ugyanis előfordulhat, hogy az alapértelmezett hitelesítőadatokat, amelyeket a gyártó megadott, nem lehet megváltoztatni. Különböző okai lehetnek annak, hogy a gyártók úgy tervezik meg eszközeiket, hogy az alapértelmezett hitelesítőadatokat a felhasználók nem tudják megváltoztatni, ilyen például a gyártás során felmerülő költségek minimalizálása, az egyszerűbb és gyorsabb működés, amely szintén elvárás feléjük.[32]

A következő sérülékenységi faktort a nem biztonságos adatkezelés jelenti. Az IoT-eszközök megfelelő működéséhez különböző adatok szükségesek, valamint a működésük során különböző adatok keletkeznek, amelyeket a biztonságos használat érdekében például titkosítással vagy hozzáférés-szabályozással kell védeni. Ilyen adatok a hitelesítőadatok, az üzenetek és a személyes adatok is, mindemellett idetartoznak a különböző parancsadatok is. Ezeknek az adatoknak a védelme kiemelt szerepet érdemel, ugyanis ezek felhasználásával különböző rosszindulatú tevékenységeket tudnak végrehajtani.[33]

A sérülékenységi faktorok közé tartozik a hitelesítési mechanizmusok hiánya, általános probléma, hogy az IoT-eszközök nem rendelkeznek hitelesítési mechanizmusokkal. A legtöbb számítógép vagy akként működő eszköz használatához hitelesítési adatokkal kell igazolnia magát a felhasználónak. Amennyiben ez nem történik meg, vagy többszöri próbálkozásra sem sikerül, a rendszer automatikusan zárolja magát, és a felhasználó nem tud belépni. Ha az IoT-eszközök rendelkeznének ilyen védelemmel, egyszerűen lehetne gondot okozni, ugyanis a hackerek a többszöri próbálkozás következtében ki tudnák zárni a felhasználókat, amivel problémákat tudnának okozni például az ipari termelés során is.[34]

A sérülékenységek között az emberi tényező is fontos szerephez jut. A biztonságot veszélyeztető hibák elkerülése végett a felhasználóknak a feladataik ellátása érdekében szükséges jogosultságokkal kell rendelkezniük. Ha minden felhasználó rendelkezne az összes jogosultsággal, egy esetleges hackertámadás esetén a behatolók el tudnák érni, hogy a szükséges intézkedéseket ne tudják megtenni. A megfelelő

[31] Boye 2019: 73.
[32] Boye 2019: 73.
[33] Boye 2019: 73.
[34] Boye 2019: 73.

szintű jogosultság kiosztása mellett fontos a felhasználók folyamatos biztonságtudatosságának növelése, oktatása a kiberbiztonsági kockázatok elkerülése érdekében.[35]

Jogosultságokkal nem csak a felhasználók rendelkeznek. Az IoT-eszközök nagy része rendelkezik internet-hozzáféréssel, amire igazából nincs is szüksége a feladatai ellátásához. Szükséges beállítani, hogy az eszközök csak azokra a feladatokra legyenek képesek, amelyekre használatuk során szükség van, hogy ne váljanak rosszindulatú tevékenység eszközévé.

A gyenge biztonsági szabályzat azt jelenti, hogy az IoT-eszközök gyártóinak irányában nincsenek felállítva megfelelő szabályok, amelyek a hibák és fenyegetések bejelentési kötelezettségére vonatkoznának. A vállalatok a legtöbb esetben nem mérik fel kellően az IoT-eszközök használatával járó veszélyeket, és nem készítenek biztonsági szabályzatot, amely az eszközök kezelésére vonatkozna.[36]

Az eszközök tervezése során előfordulhat, hogy különböző hibák léphetnek fel. Ezeknek a termékeknek a specifikációi olyan hibákat tartalmaznak, amelyek lehetőséget nyújtanak arra, hogy rosszindulatú kódok kerüljenek be az eszközökbe, amelyek lehetőséget adnak a kód készítőinek arra, hogy az eszközök az ő parancsaikat hajtsák végre, ne engedélyezzék az alapértelmezett jelszavak megváltoztatását, vagy az eszközök közötti kommunikációba avatkozzanak be. Ez nem kifejezetten hardveres hibát jelent, előfordulhat, hogy az eszköz szoftverében van a hiba. Az ilyen problémákat általánosságban egy frissítés ki tudja küszöbölni, de először lokalizálni kell a hibát.[37]

Az informatikában a számítógépekhez kapcsolható eszközök és a számítógépek portok segítségével kommunikálnak egymással a külső kapcsolattartás miatt. Megjelenési formájukat tekintve ezek lehetnek fizikai vagy logikai portok. Fizikai portok például az USB-csatlakozók. A logikai portok kezelését pedig a routerek is elvégezhetik. A portok sebezhetőségük esetén lehetőséget biztosíthatnak a rosszindulatú kódok bejutására, például egy pendrive segítségével. Ezért az eszközöknek csak a szükséges mennyiségű porttal kell rendelkezniük az ilyenfajta veszélyek elkerülése érdekében.

A kritikus komponensek elkülönítési hibái akkor jelentkeznek, ha az információkat ugyanazon rendszer kezeli. Vannak olyan információk és adatok, amelyeket külön kell kezelni, gondoljunk bele, egy vonaton az utasok számára elérhető wifihálózatnak el kell különülnie, és semmilyen formában nem csatlakozhat a vasúthálózat működéséhez kapcsolódó információkhoz.[38]

[35] Boye 2019: 73.
[36] Boye 2019: 73.
[37] Boye 2019: 73.
[38] Boye 2019: 73.

Az IoT-eszközök sok esetben nagy területen is elhelyezkedhetnek, aminek következtében kiszolgáltatottá válhatnak illetéktelen személyekkel szemben. Ennek az a veszélye, hogy tudják manipulálni az eszközöket, adott esetben ki is tudják cserélni őket.[39]

Az eszközök felszerelése és kezelése minden esetben szakértelmet igényel, egy átlag felhasználó a legtöbb esetben az alapbeállításokat tudja megváltoztatni, viszont egy szakember, aki részletesen ismeri ezeket az eszközöket, sokkal biztonságosabbá tudja tenni a használatukat.

Ha az IoT-eszközök nem megfelelően vannak konfigurálva, illetve nem hozzáértő személy készíti elő a használatukat, különféle adatvédelmi aggályok merülhetnek fel. Mivel az eszközök össze vannak kapcsolva, elérési hídként szolgálhatnak a további eszközök számára, ami kiváló lehetőséget biztosít a hackereknek, hogy szenzitív adatokat szerezzenek meg.[40]

Az eszközök eléréséhez és vezérléséhez különböző interfészekre van szükség. Ilyenek például a webes felületek, mobilapplikációk vagy a számítógépes felületek, amelyek segítségével távolról hozzá tudunk férni az adott eszközhöz. Ha ezek az interfészek nem rendelkeznek kellő védelemmel, átjáróként tudnak szolgálni a további eszközeink felé, ami szintén lehetőséget biztosít a hackerek számára, hogy a szenzitív adatainkat megszerezzék, vagy átvegyék az irányítást az eszközeink felett.

Egészségügyi intelligens eszközök

Az IoT-eszközök az egészségügy területén is forradalmi változásokat jelentettek. Különböző, a testünket figyelő eszközök jelentek meg a piacon a saját felhasználású eszközöktől kezdve az orvosi felhasználásig.

Az intelligens egészségügyi eszközök lehetnek hordozhatók és beültethetők, amelyek hatalmas előrelépést jelentenek az egészségügyi felhasználás tekintetében. Ez a technológiai fejlődés lehetőséget ad a felhasználók számára, hogy felelősséget vállaljanak egészségükért, és tudatosabban éljenek. Illetve a hordozható eszközök a krónikus betegségek kapcsán klinikai fókuszponttá válhatnak a betegek megfigyelése során.[41]

Az intelligens egészségügyi eszközöknek különböző formái ismertek. A beültethető eszközök számos egészségügyi problémát képesek megoldani. Ilyenek például az intelligens tabletták, amelyek orvosbiológiai adatokat képesek továbbítani, illetve

[39] Boye 2019: 73.
[40] Boye 2019: 73.
[41] Krohn–Metcalf–Salber 2017: 3.

képesek figyelmeztetni a beteget, hogy vegyék be a gyógyszereiket, de még számos beültethető megfigyelőberendezés létezik, amelyek képesek kezelni akár egy hirtelen bekövetkező szívrohamot is.[42]

Igaz, nem hajtottak végre ezekkel az eszközökkel támadást, de 2013-ban Richard Bruce Cheney, az Amerikai Egyesült Államok 46. alelnöke kikapcsoltatta a szívritmus-szabályozójának vezeték nélküli kapcsolatát, mert attól félt, hogy kibertámadás áldozatává fog válni. Ez ugyan elsőre furának tűnhet, de 2017-ben az Egyesült Államok Élelmiszer- és Gyógyszerügyi Hatósága több mint 500 ezer pacemakert hívott vissza, mivel attól tartottak, hogy a használók kibertámadás áldozatává válhatnak.[43]

Ezek alapján le lehet vonni azt a következtetést, hogy az intelligens egészségügyi eszközök a jövőben kifejezetten fontos részei lesznek az egészségügyi ellátásnak, de mindemellett kockázatokat rejtenek, ami egy esetleges rosszindulatú támadás esetén komoly problémát okozhat.

PÉLDA AZ IOT-ESZKÖZÖKKEL VÉGREHAJTHATÓ TÁMADÁSRA

A lent említett támadásra ugyan még nem volt példa, de kísérletekkel bebizonyították, hogy igenis kellő figyelmet kell fordítani ezen eszközök védelmére. Biztonsági kutatók, etikus hackerek és sok biztonsági szakember folyamatosan azon dolgozik, hogy feltárják a lehetséges támadási eseteket a különböző rendszerek sérülékenységei alapján.[44]

Jeep Cherokee

2015-ben a Wired nevű YouTube-csatorna tett közzé egy videót, amelyben egy Jeep Cherokee ellen hajtottak végre támadást. A videóban látható, hogy Charlie Miller és Chris Valasek hackerek nem utaznak az autóban, egy távoli ponton vannak, és mégis képesek irányítani az autó elektronikai rendszerét. A kísérlet végrehajtásakor az autóban utazó személyt felkészítették, hogy különös dolgokat fog tapasztalni az autóval kapcsolatban, szóval ne essen pánikba. Először csak az autó központi kijelzőjére vetítettek ki egy őket ábrázoló képet, majd az autó szórakoztató rendszerét, valamint az ablaktörlő lapátokat és a szélvédőmosó berendezést kezelték

[42] Krohn–Metcalf–Salber 2017: 3.
[43] Boye 2019: 73.
[44] Hanes 2017: 50.

a távolból. A nyílt úton végrehajtott kísérlet során az autó motorját is le tudták állítani, ami már kifejezetten veszélyes szituációt is tudott volna eredményezni. A további tesztek során képesek voltak az autót is irányítani, amit egy forgalomtól elzárt területen hajtottak végre. Hogy a kísérletet végre tudják hajtani, egy autót vásárolniuk kellett, hogy tanulmányozni tudják az alkatrészeit, illetve fel tudják tárni a feltörési lehetőségeket.[45] Ahhoz, hogy át tudják venni az irányítást az autó felett, nem kellett mást tenniük, mint hogy hozzácsatlakoztak a Sprint mobilhálózathoz, megkeresték a sebezhető jármű IP-címét, létrehoztak egy kapcsolatot, amelynek segítségével kártékony programokat juttattak be az autó rendszerébe. A problémát az okozta, hogy a gépjármű gyenge hitelesítési adatokkal és nem biztonságos porttal rendelkezett.

ÖSSZEGZÉS

Összegzésként elmondható, hogy bár az IoT-eszközöket kifejezetten terrortámadásra nem használták még fel, de potenciális fenyegetést jelentenek. Ezek az eszközök olyan új fegyvereket adhatnak a terroristák kezébe, amelyek a legtöbb háztartásban és ipari területen megtalálhatók. Egyedül a kreativitásukra van szükségük, ugyanis ez egy újszerű támadási formát vetít előre, amely meglepetésszerű lehet a társadalom számára.

Egy ilyen támadás kihatással lenne minden felhasználóra, ami több területen is jelentőséggel bírna, megnehezítené az eszközök felhasználását és terjedését.

FELHASZNÁLT IRODALOM

Akhgar, Babak – Staniforth, Andrew – Bosco, Francesca (2014): *Cyber Crime and Cyber Terrorism Investigator's Handbook.* Waltham: Elsevier.

Bács Zoltán György (2022): Új, innovatív módszer megalapozása az elemző-értékelő munkában. *Magyar Rendészet,* 22(3), 83–99. Online: https://doi.org/10.32577/mr.2022.3.5

Boye, Carolina A. Adaros (2019): *Understanding Cyberrisks in IoT: When Smart Things Turn Against You.* New York: Business Expert.

Elder, Jeff (2019): How Kevin Ashton Named The Internet of Things. *blog.avast.com,* 2019. augusztus 20. Online: https://blog.avast.com/kevin-ashton-named-the-internet-of-things

Hanes, David et al. (2017): *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things.* Indianapolis: Cisco Press.

[45] Hanes 2017: 50.

HENSCHKE, Adam et al. (2021): *Counter-Terrorism, Ethics and Technology.* New York: Springer Nature. Online: https://doi.org/10.1007/978-3-030-90221-6

HUSAIN, Mohammad Shahid – KHAN, Mohammad Zunnun (2020): *Critical Concepts, Standards, and Techniques in Cyber Forensics.* Hershey: IGI Global. Online: https://doi.org/10.4018/978-1-7998-1558-7

IoT Analytics (2022): *IoT 2022: Connected Devices Growing 18% to 14.4 Billion Globally.* Online: https://www.iotforall.com/state-of-iot-2022

KASZNÁR Attila (szerk.) (2017): *Bevezetés a terrorelhárítás alapjaiba.* Budapest: Dialóg Campus.

KROHN, Richard – METCALF, David – SALBER, Patricia (2017): *Connected Health.* New York: Wentworth Press. Online: https://doi.org/10.1201/9781315184494

NETANJAHU, Benjamin (1995): *Harc a terrorizmus ellen (Hogyan lehet legyőzni a nemzetközi terrorizmust).* Pécs: Alexandra.

TÓTH Gábor (2018): A *botnetek és az IoT eszközök jelentette új kihívások.* Kari Tudományos Diákköri Konferencia. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar.

Egyéb források

ENISA Threat Landscape Report 2017. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017